Nathan R. Ring
Nevada State Bar No. 12078
STRANCH, JENNINGS & GARVEY, PLLC
3100 W. Charleston Boulevard, Suite 208
Las Vegas, NV 89102
Telephone: (725) 235-9750
lasvegas@stranchlaw.com

Tyler J. Bean (*pro hac vice* forthcoming)
SIRI & GLIMSTAD LLP
745 Fifth Avenue, Suite 500
New York, New York 10151
Tel: (212) 532-1091
tbean@sirillp.com

Counsel for Plaintiff and the Proposed Class

UNITED STATES DISTRICT COURT
DISTRICT OF NEVADA

DARLENE MARTIN AND **DAVID WILLEY**, ON BEHALF OF THEMSELVES AND ALL OTHERS SIMILARLY SITUATED, PLAINTIFF, V. RIVERSIDE RESORT & CASINO, INC. AND RIVERSIDE RESORT & CASINO, LLC, DEFENDANTS.	Case No.: CLASS ACTION COMPLAINT JURY TRIAL DEMANDED

Plaintiffs Darlene Martin and David Willey ("Plaintiffs"), individually and on behalf of all similarly situated persons, allege the following against Riverside Resort and Casino, Inc. and Riverside Resort and Casino LLC (collectively, "Riverside" or "Defendant") based upon personal knowledge with respect to themselves and on information and belief derived from, among other things, investigation by Plaintiffs' counsel and review of public documents as to all other matters:

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

I. INTRODUCTION

1. Plaintiffs bring this class action against Riverside for its failure to properly secure and safeguard Plaintiffs' and other similarly situated former and current employees and customers' Name and Social Security Number (the "Private Information") from hackers.

2. Riverside owns, maintains and operates Don Laughlin's Riverside Resort Hotel & Casino ("the Resort"). The Resort, based in Laughlin, Nevada, includes an 89,000-foot casino,[1] a resort hotel with 1,350 guest rooms,[2] a six-screen movie theater,[3] and maintains a yacht for riverboat tours and for guests to charter.[4] The Resort employs almost 2,000 employees with an annual payroll of nearly $40 million.[5]

3. On or about September 5, 2024, Riverside filed official notice of a hacking incident with the Office of the Maine Attorney General. Under state law, organizations must report breaches involving Name and Social Security Numbers.

4. On or about September 4, Riverside also sent out data breach letters to individuals whose information was compromised as a result of the hacking incident.

5. Based on the Notice filed by the company, on July 25, 2024, Riverside detected unusual activity on some of its computer systems. In response, the company launched an investigation. The Riverside investigation revealed that an unauthorized party had accessed and

---

[1] *See Listing of Financial Statements Square Footage*, STATE OF NEVADA GAMING CONTROL BOARD (2015), *available at*: https://web.archive.org/web/20161225155040/http://gaming.nv.gov/modules/showdocument.aspx?documentid=3428 (last visited Sep. 12, 2024).

[2] *Hotel*, DON LAUGHLIN'S RIVERSIDE RESORT HOTEL AND CASINO, https://www.riversideresort.com/hotel-rooms-riverside/, (last visited Sep. 12, 2024).

[3] *Riverside Cinemas*, DON LAUGHLIN'S RIVERSIDE RESORT HOTEL AND CASINO, https://www.riversideresort.com/riverside-cinemas-6-plex/, (last visited Sep. 12, 2024).

[4] *USS Riverside*, DON LAUGHLIN'S RIVERSIDE RESORT HOTEL AND CASINO *https://www.riversideresort.com/uss-riverside-tours/*, (last visited Sep. 12, 2024).

[5] *History*, DON LAUGHLIN'S RIVERSIDE RESORT HOTEL AND CASINO *https://www.riversideresort.com/uss-riverside-tours/*, https://www.riversideresort.com/don-laughlin-history-founder-riverside-resort-casino/, (last visited Sep. 12, 2024).

acquired certain computer files earlier that day (the "Data Breach"). On August 9, 2024, Riverside concluded its investigation after identifying 51,555 individuals whose information had been stolen during the Data Breach.

6. Plaintiffs and "Class Members" (defined below) were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm. The risk will remain for their respective lifetimes.

7. The Private Information compromised in the Data Breach included highly sensitive data that represents a gold mine for data thieves, including but not limited to, Name and Social Security Number, that Riverside collected and maintained.

8. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including, *e.g.*, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

9. There has been no assurance offered by Riverside that all personal data or copies of data have been recovered or destroyed, or that Defendant has adequately enhanced its data security practices sufficient to avoid a similar breach of its network in the future.

10. Therefore, Plaintiffs and Class Members have suffered and are at an imminent, immediate, and continuing increased risk of suffering ascertainable losses in the form of harm from identity theft and other fraudulent misuse of their Private Information, the loss of the benefit of their bargain, out-of-pocket expenses incurred to remedy or mitigate the effects of the Data Breach, and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
STRANCH, JENNINGS & GARVEY PLLC
725-235-9750
lasvegas@stranchlaw.com

11. Plaintiffs bring this class action lawsuit to address Riverside's inadequate safeguarding of Class Members' Private Information that it collected and maintained.

12. The potential for improper disclosure and theft of Plaintiffs' and Class Members' Private Information was a known risk to Riverside, and thus Riverside was on notice that failing to take necessary steps to secure the Private Information left it vulnerable to an attack.

13. Upon information and belief, Riverside and its employees failed to properly implement security practices with regard to the computer network and systems that housed the Private Information. Had Riverside properly monitored its networks, it would have discovered the Breach sooner.

14. Plaintiffs' and Class Members' identities are now at risk because of Riverside's negligent conduct as the Private Information that Riverside collected and maintained is now in the hands of data thieves and other unauthorized third parties.

15. Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose Private Information was accessed and/or compromised during the Data Breach.

16. Accordingly, Plaintiffs, on behalf of themselves and the Class, assert claims for Negligence, Negligence *Per Se*, Breach of Implied Contract, and Unjust Enrichment.

II. PARTIES

17. Plaintiff Darlene Martin is, and at all times mentioned herein was, an individual citizen of the State of Arizona.

18. Plaintiff David Willey is, and at all times mentioned herein was, an individual citizen of the State of Nevada.

19. Riverside Resort and Casino, Inc. is a corporation incorporated in Nevada with its principal place of business at 1650 S. Casino Drive, Laughlin, NV 89029 in Clark County.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

20. Riverside Resort and Casino, LLC is a limited-liability corporation incorporated in Nevada with its principal place of business at 1650 S. Casino Drive, Laughlin, NV 89029 in Clark County.

III. JURISDICTION AND VENUE

21. The Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. Upon information and belief, the number of class members is over 100, many of whom have different citizenship from Riverside. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

22. This Court has jurisdiction over Riverside Resort and Casino, Inc. because it operates in and is incorporated in this District.

23. This Court has jurisdiction over Riverside Resort and Casino, LLC because it operates in and is incorporated in this District.

24. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District and Defendant has harmed Class Members residing in this District.

IV. FACTUAL ALLEGATIONS

A. Riverside's Business and Collection of Plaintiffs' and Class Members' Private Information

25. Defendant owns, maintains and operates Don Laughlin's Riverside Resort Hotel & Casino. The Resort, based in Laughlin, Nevada, includes an 89,000-foot casino,[6] a resort hotel with

[6] *See Listing of Financial Statements Square Footage*, STATE OF NEVADA GAMING CONTROL BOARD (2015), *available at*: https://web.archive.org/web/20161225155040/http://gaming.nv.gov/modules/showdocument.aspx?documentid=3428 (last visited Sep. 12, 2024).

3100 W. Charleston Blvd., #208 Las Vegas, NV 89102 SJG STRANCH, JENNINGS & GARVEY PLLC 725-235-9750 lasvegas@stranchlaw.com

1,350 guest rooms,[7] a six-screen movie theater,[8] and maintains a yacht for riverboat tours and for guests to charter.[9] The Resort employs almost 2,000 employees with an annual payroll of nearly $40 million.[10]

26. As a condition of employment and/or using Riverside's facilities and amenities, Riverside requires that its former and current employees and customers entrust it with highly sensitive personal information. In the ordinary course of receiving service from Riverside, Plaintiffs and Class Members were required to provide their Private Information to Defendant.

27. Riverside uses this information, *inter alia*, to manage employee benefits and hiring, confirm hotel bookings and verify identification for age-restricted gambling.

28. Because of the highly sensitive and personal nature of the information Riverside acquires and stores with respect to its customers, Riverside, upon information and belief, promises to, among other things: keep former and current employees and customers' Private Information private; comply with industry standards related to data security and the maintenance of its former and current employees and customers' Private Information; inform its former and current employees and customers of its legal duties relating to data security and comply with all federal and state laws protecting former and current employees and customers' Private Information; only use and release former and current employees and customers' Private Information for reasons that relate to the services it provides; and provide adequate notice to former and current employees and customers if their Private Information is disclosed without authorization.

---

[7] *Hotel*, DON LAUGHLIN'S RIVERSIDE RESORT HOTEL AND CASINO, https://www.riversideresort.com/hotel-rooms-riverside/, (last visited Sep. 12, 2024).

[8] *Riverside Cinemas*, DON LAUGHLIN'S RIVERSIDE RESORT HOTEL AND CASINO, https://www.riversideresort.com/riverside-cinemas-6-plex/, (last visited Sep. 12, 2024).

[9] *USS Riverside*, DON LAUGHLIN'S RIVERSIDE RESORT HOTEL AND CASINO, *https://www.riversideresort.com/uss-riverside-tours/*, (last visited Sep. 12, 2024).

[10] *History*, DON LAUGHLIN'S RIVERSIDE RESORT HOTEL AND CASINO, *https://www.riversideresort.com/uss-riverside-tours/*, https://www.riversideresort.com/don-laughlin-history-founder-riverside-resort-casino/, (last visited Sep. 12, 2024).

SJG STRANCH, JENNINGS & GARVEY PLLC
3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com

29. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, Riverside assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' Private Information from unauthorized disclosure and exfiltration.

30. Indeed, in its Privacy Policy, Riverside demonstrates that it is well aware of the importance of cybersecurity, stating:[11]

> Non-Personal Information and Personal Information, including Confidential Personal Information, collected by the Riverside Resort and Casino web site and the Riverside Resort and Casino is stored on secure servers. The secure servers are protected by firewalls and a multitude of other industry standard security measures. These security measures are instituted to ensure the protection of these secure servers from unauthorized access….
>
> Our staff is required to take reasonable measures to ensure that unauthorized persons cannot view or access your Personal Information. Employees who violate our privacy policies are subject to disciplinary action, up to and including termination…
>
> As a standard security practice, we will take reasonable steps, which are standard in the industry to ensure that the communication methods used to support the Riverside Resort and Casino do not permit connection or communication by methods that have known security weaknesses or vulnerabilities

31. Plaintiffs and Class Members relied on Riverside to keep their Private Information confidential and securely maintained and to only make authorized disclosures of this information, which Defendant ultimately failed to do.

B. <u>The Data Breach and Riverside's Inadequate Notice to Plaintiffs and Class Members</u>

32. According to Defendant's Notice, it learned of unauthorized access to its computer systems on the day of the Data Breach, July 25, 2024.

---

[11] *Privacy Policy*, DON LAUGHLIN'S RIVERSIDE RESORT HOTEL AND CASINO, https://www.riversideresort.com/privacy-policy//, (last visited Sep. 12, 2024).

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

33. Through the Data Breach, the unauthorized cybercriminal(s) accessed a cache of highly sensitive Private Information, including Names and Social Security Numbers,

34. On or about September 9, 2024, roughly two months after Riverside learned that the Class's Private Information was first accessed by cybercriminals, Riverside finally began to notify impacted individuals that its investigation determined that their Private Information was accessed and acquired.

35. Riverside delivered Data Breach Notification Letters to Plaintiffs and Class Members, alerting them that their highly sensitive Private Information had been exposed in a "data security incident."

36. The notice letter then attached some pages entitled "Steps You Can Take to Help Protect Your Information," which listed generic steps that victims of data security incidents can take, such as getting a copy of a credit report or notifying law enforcement about suspicious financial account activity. Other than providing one year of crediting monitoring that Plaintiffs and Class Members would have to affirmatively sign up for and a call center number that victims could contact "with any questions," Riverside offered no other substantive steps to help victims like Plaintiffs and Class Members to protect themselves. On information and belief, Riverside sent a similar generic letter to all individuals affected by the Data Breach.

37. Riverside had obligations created by contract, industry standards, common law, and representations made to Plaintiffs and Class Members to keep Plaintiffs' and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

38. Plaintiffs and Class Members provided their Private Information to Riverside with the reasonable expectation and mutual understanding that Riverside would comply with its obligations to keep such information confidential and secure from unauthorized access and to provide timely notice of any security breaches.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

39. Riverside's data security obligations were particularly important given the substantial increase in cyberattacks in recent years, especially within the gambling industry. Casinos have become such a common target for cybercriminals that the Federal Bureau of Investigation ("FBI") released a bulletin only last year highlighting the need for casinos to prioritize data security.[12]

40. Riverside knew or should have known that its electronic records would be targeted by cybercriminals.

C. Riverside Failed to Comply with FTC Guidelines

41. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making. Indeed, the FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

42. In October 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep, properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand their network's vulnerabilities, and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to

[12] *Private Industry Notification*, FEDERAL BUREAU OF INVESTIGATION (Nov. 7, 2023), available online at: https://www.aha.org/system/files/media/file/2023/11/bi-tlp-clear-pin-ransomware-actors-continue-to-gain-access-through-third-parties-and-legitimate-system-tools-11-7-23.pdf.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
SJG STRANCH, JENNINGS & GARVEY PLLC
725-235-9750
lasvegas@stranchlaw.com

expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone is attempting to hack into the system, watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of a breach.

43. The FTC further recommends that companies not maintain personally identifiable information ("PII") longer than is needed for authorization of a transaction, limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor the network for suspicious activity, and verify that third-party service providers have implemented reasonable security measures.

44. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data by treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by the FTCA. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

45. As evidenced by the Data Breach, Riverside failed to properly implement basic data security practices. Riverside's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiffs' and Class Members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

46. Riverside was at all times fully aware of its obligation to protect the Private Information of its customers yet failed to comply with such obligations. Defendant was also aware of the significant repercussions that would result from its failure to do so.

D. Riverside Failed to Comply with Industry Standards

47. As noted above, experts studying cybersecurity routinely identify businesses as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

48. Some industry best practices that should be implemented by businesses like Riverside include but are not limited to educating all employees, strong password requirements, multilayer security including firewalls, anti-virus and anti-malware software, encryption, multi-factor authentication, backing up data, and limiting which employees can access sensitive data. As evidenced by the Data Breach, Defendant failed to follow some or all of these industry best practices.

49. Other best cybersecurity practices that are standard in the industry include: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; and training staff regarding these points. As evidenced by the Data Breach, Defendant failed to follow these cybersecurity best practices.

50. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

51. Defendant failed to comply with these accepted standards, thereby permitting the Data Breach to occur.

E. Riverside Breached its Duty to Safeguard Plaintiffs' and Class Members' Private Information

52. In addition to its obligations under federal and state laws, Riverside owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

compromised, lost, stolen, accessed, and misused by unauthorized persons. Riverside owed a duty to Plaintiffs and Class Members to provide reasonable security, including complying with industry standards and requirements, training for its staff, and ensuring that its computer systems, networks, and protocols adequately protected the Private Information of Class Members

53. Riverside breached its obligations to Plaintiffs and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. Riverside's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system that would reduce the risk of data breaches and cyberattacks;

b. Failing to adequately protect its former and current employees and customers' Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to sufficiently train its employees regarding the proper handling of its former and current employees and customers Private Information;

e. Failing to fully comply with FTC guidelines for cybersecurity in violation of the FTCA;

f. Failing to adhere to industry standards for cybersecurity as discussed above; and

g. Otherwise breaching its duties and obligations to protect Plaintiffs' and Class Members' Private Information.

54. Riverside negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' Private Information by allowing cyberthieves to access its computer network and systems which contained unsecured and unencrypted Private Information.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

55. Had Riverside remedied the deficiencies in its information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, it could have prevented intrusion into its information storage and security systems and, ultimately, the theft of Plaintiffs' and Class Members' confidential Private Information.

56. Accordingly, Plaintiffs' and Class Members' lives were severely disrupted. What's more, they have been harmed as a result of the Data Breach and now face an increased risk of future harm that includes, but is not limited to, fraud and identity theft. Plaintiffs and Class Members also lost the benefit of the bargain they made with Riverside.

F. Riverside Should Have Known that Cybercriminals Target Private Information to Carry Out Fraud and Identity Theft

57. The FTC hosted a workshop to discuss "informational injuries," which are injuries that consumers like Plaintiffs and Class Members suffer from privacy and security incidents such as data breaches or unauthorized disclosure of data.[13] Exposure of highly sensitive personal information that a consumer wishes to keep private may cause harm to the consumer, such as the ability to obtain or keep employment. Consumers' loss of trust in e-commerce also deprives them of the benefits provided by the full range of goods and services available which can have negative impacts on daily life.

58. Any victim of a data breach is exposed to serious ramifications regardless of the nature of the data that was breached. Indeed, the reason why criminals steal information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity

[13] *FTC Information Injury Workshop, BE and BCP Staff Perspective,* Federal Trade Commission, (October 2018), *available at* https://www.ftc.gov/system/files/documents/reports/ftc-informational-injury-workshop-be-bcp-staff-perspective/informational_injury_workshop_staff_report_-_oct_2018_0.pdf (last visited on Sep. 12, 2024).

3100 W. Charleston Blvd., #208 Las Vegas, NV 89102 SJG STRANCH, JENNINGS & GARVEY PLLC 725-235-9750 lasvegas@stranchlaw.com

thieves who desire to extort and harass victims or to take over victims' identities in order to engage in illegal financial transactions under the victims' names.

59. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity or to otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

60. In fact, as technology advances, computer programs may scan the Internet with a wider scope to create a mosaic of information that may be used to link compromised information to an individual in ways that were not previously possible. This is known as the "mosaic effect." Names and dates of birth, combined with contact information like telephone numbers and email addresses, are very valuable to hackers and identity thieves as it allows them to access users' other accounts.

61. Thus, even if certain information was not purportedly involved in the Data Breach, the unauthorized parties could use Plaintiffs' and Class Members' Private Information to access accounts, including, but not limited to, email accounts and financial accounts, to engage in a wide variety of fraudulent activity against Plaintiffs and Class Members.

62. One such example of this is the development of "Fullz" packages.

63. Cybercriminals can cross-reference two sources of the Private Information compromised in the Data Breach to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

dossiers on individuals. These dossiers are known as "Fullz" packages.

64. The development of "Fullz" packages means that the stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiffs' and the proposed Class's phone numbers, email addresses, and other sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card or financial account numbers may not be included in the Private Information stolen in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiffs and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiffs and other Class Members' stolen Private Information are being misused, and that such misuse is fairly traceable to the Data Breach.

65. For these reasons, the FTC recommends that identity theft victims take several time-consuming steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert on their account (and an extended fraud alert that lasts for 7 years if someone steals the victim's identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a freeze on their credit, and correcting their credit reports.[14] However, these steps do not guarantee protection from identity theft but can only mitigate identity theft's long-lasting negative impacts.

66. Identity thieves can also use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, bank fraud, to obtain a driver's license or official identification card in the ***victim's*** name but with the thief's picture, to obtain government benefits, or to file a fraudulent tax return using the victim's

[14] *See IdentityTheft.gov,* Federal Trade Commission, *available at* https://www.identitytheft.gov/Steps (last visited Sep. 12, 2024).

3100 W. Charleston Blvd., #208 Las Vegas, NV 89102 SJG STRANCH, JENNINGS & GARVEY PLLC 725-235-9750 lasvegas@stranchlaw.com

information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house in the victim's name, receive medical services in the victim's name, and even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

67. PII is data that can be used to detect a specific individual. PII is a valuable property right. Its value is axiomatic, considering the value of big ***data*** in corporate America and the consequences of cyber thefts (which include heavy prison sentences). Even this obvious risk-to-reward analysis illustrates beyond doubt that PII has considerable market value.

68. The U.S. Attorney General stated in 2020 that consumers' sensitive personal information commonly stolen in data breaches "has economic value."[15] The increase in cyberattacks, and attendant risk of future attacks, was widely known and completely foreseeable to the public and to anyone in Defendant's industry.

69. The PII of consumers remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, PII can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[16] Experian reports that a stolen credit or debit card number can sell

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

[15] *See Attorney General William P. Barr Announces Indictment of Four Members of China's Military for Hacking into Equifax*, U.S. Dep't of Justice, Feb. 10, 2020, available at https://www.justice.gov/opa/speech/attorney-general-william-p-barr-announces-indictment-fourmembers-china-s-military (last visited on Sep. 12, 2024).

[16] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited on Sep. 12, 2024).

for $5 to $110 on the dark web and that the "*fullz*" (a term criminals who steal credit card information use to refer to a complete set of information on a fraud victim) sold for $30 in 2017.[17]

70. Furthermore, even information such as names, email addresses and phone numbers, can have value to a hacker. Beyond things like spamming customers, or launching phishing attacks using their names and emails, hackers, *inter alia*, can combine this information with other hacked data to build a more complete picture of an individual. It is often this type of piecing together of a puzzle that allows hackers to successfully carry out phishing attacks or social engineering attacks. This is reflected in recent reports, which warn that "[e]mail addresses are extremely valuable to threat actors who use them as part of their threat campaigns to compromise accounts and send phishing emails."[18]

71. The Dark Web Price Index of 2022, published by PrivacyAffairs[19] shows how valuable just email addresses alone can be, even when not associated with a financial account:

Email Database Dumps	Avg. Price USD (2022)
10,000,000 USA email addresses	$120
600,000 New Zealand email addresses	$110
2,400,000 million Canada email addresses	$100

[17] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited on Sep. 12, 2024).

[18] *See* https://www.magicspam.com/blog/dark-web-price-index-the-cost-of-email-data/ (last visited on Sep. 12, 2024).

[19] *See* https://www.privacyaffairs.com/dark-web-price-index-2022/ (last visited on Sep. 12, 2024).

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

72. Beyond using email addresses for hacking, the sale of a batch of illegally obtained email addresses can lead to increased spam emails. If an email address is swamped with spam, that address may become cumbersome or impossible to use, making it less valuable to its owner.

73. Likewise, the value of PII is increasingly evident in our digital economy. Many companies including Riverside collect PII for purposes of data analytics and marketing. These companies, collect it to better target customers, and shares it with third parties for similar purposes.[20]

74. One author has noted: "Due, in part, to the use of PII in marketing decisions, commentators are conceptualizing PII as a commodity. Individual data points have concrete value, which can be traded on what is becoming a burgeoning market for PII."[21]

75. Consumers also recognize the value of their personal information and offer it in exchange for goods and services. The value of PII can be derived not only by a price at which consumers or hackers actually seek to sell it, but rather by the economic benefit consumers derive from being able to use it and control the use of it.

76. A consumer's ability to use their PII is encumbered when their identity or credit profile is infected by misuse or fraud. For example, a consumer with false or conflicting information on their credit report may be denied credit. Also, a consumer may be unable to open an electronic account where their email address is already associated with another user. In this sense, among others, the theft of PII in the Data Breach led to a diminution in value of the PII.

77. Data breaches, like that at issue here, damage consumers by interfering with their fiscal autonomy. Any past and potential future misuse of Plaintiffs' PII impairs their ability to participate in the economic marketplace.

---

[20] *See* https://robinhood.com/us/en/support/articles/privacy-policy/ (last visited on Sep. 12, 2024).

[21] *See* John T. Soma, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ('PII') Equals the "Value" of Financial Assets,* 15 Rich. J. L. & Tech. 11, 14 (2009).

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

78. It must also be noted that there may be a substantial time lag between when harm occurs and when it is discovered, and also between when PII and/or personal financial information is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:[22]

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

79. PII is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black market" for years.

80. As a result, Plaintiffs and Class Members are at an increased risk of fraud and identity theft for many years into the future. Thus, Plaintiffs and Class Members have no choice but to vigilantly monitor their accounts for many years to come.

G. Plaintiffs' and Class Members' Damages

Plaintiff Darlene Martin's Experience

81. Plaintiff Martin became a customer of Riverside prior to the data breach by using its gambling facilities.

82. When Plaintiff Martin first became a customer, Riverside required Plaintiff Martin provide it with substantial amounts of her PII.

83. On or about September 5, 20235, Plaintiff Martin received a letter entitled which told her that her Private Information had been accessed and acquired during the Data Breach. The notice

[22] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO (June 2007), *available at* https://www.gao.gov/assets/270/262904.html (last visited Sep. 12, 2024).

3100 W. Charleston Blvd., #208 Las Vegas, NV 89102 SJG STRANCH, JENNINGS & GARVEY PLLC 725-235-9750 lasvegas@stranchlaw.com

letter informed her that the Private Information compromised included her "Name and Social Security Number."

84. The notice letter offered Plaintiff Martin only one year of credit monitoring services. One year of credit monitoring is not sufficient given that Plaintiff Martin will now experience a lifetime of increased risk of identity theft and other forms of targeted fraudulent misuse of her Private Information.

85. Plaintiff Martin suffered actual injury in the form of time spent dealing with the Data Breach and the increased risk of fraud resulting from the Data Breach and/or monitoring her accounts for fraud.

86. Plaintiff Martin would not have provided her Private Information to Defendant had Defendant timely disclosed that its systems lacked adequate computer and data security practices to safeguard its customer's personal information from theft, and that those systems were subject to a data breach.

87. Plaintiff Martin suffered actual injury in the form of having her Private Information compromised and/or stolen as a result of the Data Breach.

88. Plaintiff Martin suffered actual injury in the form of damages to and diminution in the value of her personal and financial information – a form of intangible property that Plaintiff Martin entrusted to Defendant for the purpose of using their facilities, and which was compromised in, and as a result of, the Data Breach.

89. Plaintiff Martin suffered imminent and impending injury arising from the substantially increased risk of future fraud, identity theft, and misuse posed by her Private Information being placed in the hands of criminals.

90. Plaintiff Martin has a continuing interest in ensuring that her Private Information, which remains in the possession of Defendant, is protected and safeguarded from future breaches.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

91. As a result of the Data Breach, Plaintiff Martin made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing financial accounts for any indications of actual or attempted identity theft or fraud, and researching the credit monitoring offered by Defendant, as well as long-term credit monitoring options she will now need to use. Plaintiff Martin has spent several hours dealing with the Data Breach, valuable time she otherwise would have spent on other activities.

92. As a result of the Data Breach, Plaintiff Martin has suffered anxiety as a result of the release of her Private Information to cybercriminals, which Private Information she believed would be protected from unauthorized access and disclosure. These feelings include anxiety about unauthorized parties viewing, selling, and/or using her Private Information for purposes of committing cyber and other crimes against her. Plaintiff Martin is very concerned about this increased, substantial, and continuing risk, as well as the consequences that identity theft and fraud resulting from the Data Breach will have on her life.

93. Plaintiff Martin also suffered actual injury as a result of the Data Breach in the form of (a) damage to and diminution in the value of her Private Information, a form of property that Defendant obtained from Plaintiff Martin; (b) violation of her privacy rights; and (c) present, imminent, and impending injury arising from the increased risk of identity theft, and fraud she now faces.

94. As a result of the Data Breach, Plaintiff Martin anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the many harms caused by the Data Breach.

Plaintiff David Willey's Experience

95. Plaintiff Willey worked as an employee of Riverside prior to the data breach.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

96. When Plaintiff Willey first became a employee, Riverside required Plaintiff Willey provide it with substantial amounts of his PII.

97. On or about September 5, 20235, Plaintiff Willey received a letter entitled which told him that his Private Information had been accessed and acquired during the Data Breach. The notice letter informed him that the Private Information compromised included his "Name and Social Security Number."

98. The notice letter offered Plaintiff Willey only one year of credit monitoring services. One year of credit monitoring is not sufficient given that Plaintiff Willey will now experience a lifetime of increased risk of identity theft and other forms of targeted fraudulent misuse of his Private Information.

99. Plaintiff Willey suffered actual injury in the form of time spent dealing with the Data Breach and the increased risk of fraud resulting from the Data Breach and/or monitoring his accounts for fraud.

100. Plaintiff Willey would not have provided his Private Information to Defendant had Defendant timely disclosed that its systems lacked adequate computer and data security practices to safeguard its employee's personal information from theft, and that those systems were subject to a data breach.

101. Plaintiff Willey suffered actual injury in the form of having his Private Information compromised and/or stolen as a result of the Data Breach.

102. Plaintiff Willey suffered actual injury in the form of damages to and diminution in the value of his personal and financial information – a form of intangible property that Plaintiff Willey entrusted to Defendant for the purpose of using their facilities, and which was compromised in, and as a result of, the Data Breach.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

103. Plaintiff Willey suffered imminent and impending injury arising from the substantially increased risk of future fraud, identity theft, and misuse posed by his Private Information being placed in the hands of criminals.

104. Plaintiff Willey has a continuing interest in ensuring that his Private Information, which remains in the possession of Defendant, is protected and safeguarded from future breaches.

105. As a result of the Data Breach, Plaintiff Willey made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing financial accounts for any indications of actual or attempted identity theft or fraud, and researching the credit monitoring offered by Defendant, as well as long-term credit monitoring options he will now need to use. Plaintiff Willey has spent several hours dealing with the Data Breach, valuable time he otherwise would have spent on other activities.

106. As a result of the Data Breach, Plaintiff Willey has suffered anxiety as a result of the release of his Private Information to cybercriminals, which Private Information he believed would be protected from unauthorized access and disclosure. These feelings include anxiety about unauthorized parties viewing, selling, and/or using his Private Information for purposes of committing cyber and other crimes against him. Plaintiff Willey is very concerned about this increased, substantial, and continuing risk, as well as the consequences that identity theft and fraud resulting from the Data Breach will have on his life.

107. Plaintiff Willey also suffered actual injury as a result of the Data Breach in the form of (a) damage to and diminution in the value of his Private Information, a form of property that Defendant obtained from Plaintiff Willey; (b) violation of his privacy rights; and (c) present, imminent, and impending injury arising from the increased risk of identity theft, and fraud she now faces.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
STRANCH, JENNINGS & GARVEY PLLC
725-235-9750
lasvegas@stranchlaw.com

108. As a result of the Data Breach, Plaintiff Willey anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the many harms caused by the Data Breach.

109. In sum, Plaintiffs and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

110. Plaintiffs and Class Members entrusted their Private Information to Defendant in order to receive Defendant's services.

111. Plaintiffs' Private Information was subsequently compromised as a direct and proximate result of the Data Breach, which Data Breach resulted from Defendant's inadequate data security practices.

112. As a direct and proximate result of Riverside's actions and omissions, Plaintiffs and Class Members have been harmed and are at an imminent, immediate, and continuing increased risk of harm, including but not limited to, having medical services billed in their names, loans opened in their names, tax returns filed in their names, utility bills opened in their names, credit card accounts opened in their names, and other forms of identity theft.

113. Further, as a direct and proximate result of Riverside's conduct, Plaintiffs and Class Members have been forced to spend time dealing with the effects of the Data Breach.

114. Plaintiffs and Class Members also face a substantial risk of being targeted in future phishing, data intrusion, and other illegal schemes through the misuse of their Private Information, since potential fraudsters will likely use such Private Information to carry out such targeted schemes against Plaintiffs and Class Members.

115. The Private Information maintained by and stolen from Defendant's systems, combined with publicly available information, allows nefarious actors to assemble a detailed

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

mosaic of Plaintiffs and Class Members, which can also be used to carry out targeted fraudulent schemes against Plaintiffs and Class Members.

116. Plaintiffs and Class Members also lost the benefit of the bargain they made with Riverside. Plaintiffs and Class Members overpaid for services that were intended to be accompanied by adequate data security but were not. Indeed, part of the price Plaintiffs and Class Members paid to Riverside was intended to be used by Riverside to fund adequate security of Riverside's system and protect Plaintiffs' and Class Members' Private Information. Thus, Plaintiffs and the Class did not receive what they paid for.

117. Additionally, as a direct and proximate result of Riverside's conduct, Plaintiffs and Class Members have also been forced to take the time and effort to mitigate the actual and potential impact of the data breach on their everyday lives, including placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

118. Plaintiffs and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

119. Additionally, Plaintiffs and Class Members also suffered a loss of value of their PII and PHI when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases. An active and robust legitimate marketplace for Private Information also exists. In 2019, the data brokering industry was worth

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

roughly $200 billion.[23] In fact, consumers who agree to provide their web browsing history to the Nielsen Corporation can in turn receive up to $50 a year.[24]

120. As a result of the Data Breach, Plaintiffs' and Class Members' Private Information, which has an inherent market value in both legitimate and illegal markets, has been harmed and diminished due to its acquisition by cybercriminals. This transfer of valuable information happened with no consideration paid to Plaintiffs or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is apparently readily available to others, and the rarity of the Private Information has been destroyed because it is no longer only held by Plaintiffs and the Class Members, and because that data no longer necessarily correlates only with activities undertaken by Plaintiffs and the Class Members, thereby causing additional loss of value.

121. Plaintiffs and Class Members were also damaged via benefit-of-the-bargain damages. The contractual bargain entered into between Plaintiffs and Heartland included Defendant's contractual obligation to provide adequate data security, which Defendant failed to provide. Thus, Plaintiffs and Class Members did not get what they bargained for.

122. Finally, Plaintiffs and Class Members have suffered or will suffer actual injury as a direct and proximate result of the Data Breach in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach. These losses include, but are not limited to, the following:

a. Monitoring for and discovering fraudulent charges;

b. Canceling and reissuing credit and debit cards;

---

[23] *See* https://thequantumrecord.com/blog/data-brokers-profit-from-our-data/#:~:text=The%20business%20of%20data%20brokering,annual%20revenue%20of%20%24200%20billion. (last visited on August 9, 2023).

[24] *Frequently Asked Questions,* Nielsen Computer & Mobile Panel, https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last visited Jan. 16, 2023).

3100 W. Charleston Blvd., #208 Las Vegas, NV 89102 SJG STRANCH, JENNINGS & GARVEY PLLC 725-235-9750 lasvegas@stranchlaw.com

c. Addressing their inability to withdraw funds linked to compromised accounts;

d. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

e. Spending time on the phone with or at a financial institution to dispute fraudulent charges;

f. Contacting financial institutions and closing or modifying financial accounts;

g. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;

h. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised cards that had to be cancelled; and

i. Closely reviewing and monitoring bank accounts and credit reports for additional unauthorized activity for years to come.

123. Moreover, Plaintiffs and Class Members have an interest in ensuring that their Private Information, which is believed to still be in the possession of Riverside, is protected from future additional breaches by the implementation of more adequate data security measures and safeguards, including but not limited to, ensuring that the storage of data or documents containing personal and financial information is not accessible online, that access to such data is password-protected, and that such data is properly encrypted.

124. As a direct and proximate result of Riverside's actions and inactions, Plaintiffs and Class Members have suffered a loss of privacy and have suffered cognizable harm, including an imminent and substantial future risk of harm, in the forms set forth above.

V. CLASS ACTION ALLEGATIONS

125. Plaintiffs bring this action individually and on behalf of all other persons similarly situated, pursuant to Federal Rule of Civil Procedure 23(a), 23(b)(1), 23(b)(2), and 23(b)(3).

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

126. Specifically, Plaintiffs propose the following Nationwide Class, as well as the following State Subclass definitions (also collectively referred to herein as the "Class"), subject to amendment as appropriate:

Nationwide Class

All individuals in the United States who had Private Information accessed and/or acquired as a result of the Data Breach, including all who were sent a notice of the Data Breach.

Nevada Subclass

All residents of Nevada who had Private Information accessed and/or acquired as a result of the Data Breach, including all who were sent a notice of the Data Breach.

127. Excluded from the Class are Defendant and its parents or subsidiaries, any entities in which it has a controlling interest, as well as its officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded is any Judge to whom this case is assigned as well as their judicial staff and immediate family members.

128. Plaintiffs reserve the right to modify or amend the definitions of the proposed Nationwide Class, as well as the Nevada Subclass before the Court determines whether certification is appropriate.

129. The proposed Class meets the criteria for certification under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3).

130. Numerosity. The Class Members are so numerous that joinder of all members is impracticable. Though the exact number and identities of Class Members are unknown at this time, based on information and belief, the Class consists of 55,155 customers and employees of Riverside whose data was compromised in the Data Breach. The identities of Class Members are ascertainable through Riverside's records, Class Members' records, publication notice, self-identification, and other means.

3100 W. Charleston Blvd., #208 Las Vegas, NV 89102 SJG STRANCH, JENNINGS & GARVEY PLLC 725-235-9750 lasvegas@stranchlaw.com

131. Commonality. There are questions of law and fact common to the Class which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Riverside engaged in the conduct alleged herein;

b. When Riverside learned of the Data Breach;

c. Whether Riverside's response to the Data Breach was adequate;

d. Whether Riverside unlawfully lost or disclosed Plaintiffs' and Class Members' Private Information;

e. Whether Riverside failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Private Information compromised in the Data Breach;

f. Whether Riverside's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

g. Whether Riverside's data security systems prior to and during the Data Breach were consistent with industry standards;

h. Whether Riverside owed a duty to Class Members to safeguard their Private Information;

i. Whether Riverside breached its duty to Class Members to safeguard their Private Information;

j. Whether hackers obtained Class Members' Private Information via the Data Breach;

k. Whether Riverside had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiffs and the Class Members;

l. Whether Riverside breached its duty to provide timely and accurate notice of the Data Breach to Plaintiffs and Class Members;

3100 W. Charleston Blvd., #208 Las Vegas, NV 89102 SJG STRANCH, JENNINGS & GARVEY PLLC 725-235-9750 lasvegas@stranchlaw.com

m. Whether Riverside knew or should have known that its data security systems and monitoring processes were deficient;

n. What damages Plaintiffs and Class Members suffered as a result of Riverside's misconduct;

o. Whether Riverside's conduct was negligent;

p. Whether Riverside's conduct was *per se* negligent;

q. Whether Riverside was unjustly enriched;

r. Whether Plaintiffs and Class Members are entitled to actual and/or statutory damages;

s. Whether Plaintiffs and Class Members are entitled to additional credit or identity monitoring and monetary relief; and

t. Whether Plaintiffs and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

132. Typicality. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' Private Information, like that of every other Class Member, was compromised in the Data Breach.

133. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of Class Members. Plaintiffs' counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

134. Predominance. Riverside has engaged in a common course of conduct toward Plaintiffs and Class Members in that all of Plaintiffs' and Class Members' data was stored on the same computer systems and unlawfully accessed and exfiltrated in the same way. The common issues arising from Riverside's conduct affecting Class Members set out above predominate over

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

135. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Riverside. In contrast, conducting this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

136. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2). Riverside has acted and/or refused to act on grounds generally applicable to the Class such that final injunctive relief and/or corresponding declaratory relief is appropriate as to the Class as a whole.

137. Finally, all members of the proposed Class are readily ascertainable. Riverside has access to the names and addresses and/or email addresses of Class Members affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Riverside.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
SJG STRANCH, JENNINGS & GARVEY PLLC
725-235-9750
lasvegas@stranchlaw.com

VI. CLAIMS FOR RELIEF

COUNT I
NEGLIGENCE
(On behalf of Plaintiffs and the Nationwide Class or Alternatively the Nevada)

138. Plaintiffs restate and reallege all of the allegations stated above and hereafter as if fully set forth herein.

139. Riverside knowingly collected, came into possession of, and maintained Plaintiffs' and Class Members' Private Information, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such

140. Riverside knew or should have known of the risks inherent in collecting the Private Information of Plaintiffs and Class Members and the importance of adequate security. Riverside was on notice because, on information and belief, it knew or should have known that it would be an attractive target for cyberattacks.

141. Riverside owed a duty of care to Plaintiffs and Class Members whose Private Information was entrusted to it. Riverside's duties included, but were not limited to, the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Private Information in its possession;

b. To protect former and current employees and customers' Private Information using reasonable and adequate security procedures and systems compliant with industry standards;

c. To have procedures in place to prevent the loss or unauthorized dissemination of Private Information in its possession;

d. To employ reasonable security measures and otherwise protect the Private Information of Plaintiffs and Class Members pursuant to the FTCA;

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

e. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches; and

f. To promptly notify Plaintiffs and Class Members of the Data Breach, and to precisely disclose the type(s) of information compromised.

142. Riverside's duty to employ reasonable data security measures arose, in part, under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

143. Riverside's duty also arose because Defendant was bound by industry standards to protect its former and current employees and customers' confidential Private Information.

144. Plaintiffs and Class Members were foreseeable victims of any inadequate security practices on the part of Defendant, and Riverside owed them a duty of care to not subject them to an unreasonable risk of harm.

145. Riverside, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiffs' and Class Members' Private Information within Riverside's possession.

146. Riverside, by its actions and/or omissions, breached its duty of care by failing to provide, or acting with reckless disregard for, fair, reasonable, or adequate computer systems and data security practices to safeguard the Private Information of Plaintiffs and Class Members.

147. Riverside, by its actions and/or omissions, breached its duty of care by failing to promptly identify the Data Breach and then failing to provide prompt notice of the Data Breach to the persons whose Private Information was compromised.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

148. Riverside breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of its networks and systems;

c. Failing to periodically ensure that its email system maintained reasonable data security safeguards;

d. Allowing unauthorized access to Class Members' Private Information;

e. Failing to comply with the FTCA;

149. Riverside had a special relationship with Plaintiffs and Class Members. Plaintiffs' and Class Members' willingness to entrust Riverside with their Private Information was predicated on the understanding that Riverside would take adequate security precautions. Moreover, only Riverside had the ability to protect its systems (and the Private Information that it stored on them) from attack.

150. Riverside's breach of duties owed to Plaintiffs and Class Members caused Plaintiffs' and Class Members' Private Information to be compromised, exfiltrated, as alleged herein.

151. Riverside's breaches of duty also caused a substantial, imminent risk to Plaintiffs and Class Members of identity theft, loss of control over their Private Information, and/or loss of time and money to monitor their accounts for fraud.

152. As a result of Riverside's negligence in breach of its duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members are in danger of imminent harm in that their Private Information, which is still in the possession of third parties, will be used for fraudulent purposes.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

153. Riverside also had independent duties under state laws that required it to reasonably safeguard Plaintiffs' and Class Members' Private Information and promptly notify them about the Data Breach.

154. As a direct and proximate result of Riverside's negligent conduct, Plaintiffs and Class Members have suffered damages as alleged herein and are at imminent risk of further harm.

155. The injury and harm that Plaintiffs and Class Members suffered was reasonably foreseeable.

156. Plaintiffs and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

157. In addition to monetary relief, Plaintiffs and Class Members are also entitled to injunctive relief requiring Riverside to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

COUNT II
NEGLIGENCE *PER SE*
(On behalf of Plaintiffs and the Nationwide Class or Alternatively the Nevada)

158. Plaintiffs restate and reallege all of the allegations stated above and hereafter as if fully set forth herein.

159. Pursuant to Section 5 of the FTCA, Riverside had a duty to provide fair and adequate computer systems and data security to safeguard the Private Information of Plaintiffs and Class Members.

160. Riverside breached its duties by failing to employ industry-standard cybersecurity measures in order to comply with the FTCA, including but not limited to proper segregation, access controls, password protection, encryption, intrusion detection, secure destruction of unnecessary data, and penetration testing.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

161. Plaintiffs and Class Members are within the class of persons that the FTCA is intended to protect.

162. The FTCA prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice of failing to use reasonable measures to protect PII (such as the Private Information compromised in the Data Breach). The FTC rulings and publications described above, together with the industry-standard cybersecurity measures set forth herein, form part of the basis of Riverside's duty in this regard.

163. Riverside violated the FTCA by failing to use reasonable measures to protect the Private Information of Plaintiffs and the Class and by not complying with applicable industry standards, as described herein.

164. It was reasonably foreseeable, particularly given the growing number of data breaches of Private Information, that the failure to reasonably protect and secure Plaintiffs' and Class Members' Private Information in compliance with applicable laws would result in an unauthorized third-party gaining access to Riverside's networks, databases, and computers that stored Plaintiffs' and Class Members' unencrypted Private Information.

165. Riverside's violations of the FTCA constitute negligence *per se*.

166. Plaintiffs' and Class Members' Private Information constitutes personal property that was stolen due to Riverside's negligence, resulting in harm, injury, and damages to Plaintiffs and Class Members.

167. As a direct and proximate result of Riverside's negligence *per se*, Plaintiffs and the Class have suffered, and continue to suffer, injuries and damages arising from the unauthorized access of their Private Information, and the lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives.

SJG STRANCH, JENNINGS & GARVEY PLLC
3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com

168. Riverside breached its duties to Plaintiffs and the Class under the FTCA by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

169. As a direct and proximate result of Riverside's negligent conduct, Plaintiffs and Class Members have suffered injury and are entitled to compensatory and consequential damages in an amount to be proven at trial.

170. In addition to monetary relief, Plaintiffs and Class Members are also entitled to injunctive relief requiring Riverside to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

COUNT III
BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiffs and the Nationwide Class or Alternatively Nevada Subclass)

171. Plaintiffs restate and reallege all of the allegations stated above and hereafter as if fully set forth herein.

172. This Count is pleaded in the alternative to Count III above.

173. Riverside provides entertainment, lodging, and gaming services to Plaintiffs and Class Members. Plaintiffs and Class Members formed an implied contract with Defendant regarding the provision of those services through their collective conduct, including by Plaintiffs and Class Members paying for goods and services from Defendant.

174. Through Defendant's sale of goods and services, it knew or should have known that it must protect Plaintiffs' and Class Members' confidential Private Information in accordance with Riverside's policies, practices, and applicable law.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
SJG STRANCH, JENNINGS & GARVEY PLLC
725-235-9750
lasvegas@stranchlaw.com

175. As consideration, Plaintiffs and Class Members paid money to Riverside and turned over valuable Private Information to Riverside. Accordingly, Plaintiffs and Class Members bargained with Riverside to securely maintain and store their Private Information.

176. Riverside accepted possession of Plaintiffs' and Class Members' Private Information for the purpose of providing goods and services to Plaintiffs and Class Members.

177. In delivering their Private Information to Riverside and paying for goods and services, Plaintiffs and Class Members intended and understood that Riverside would adequately safeguard the Private Information as part of that service.

178. Defendant's implied promises to Plaintiffs and Class Members include, but are not limited to, (1) taking steps to ensure that anyone who is granted access to Private Information also protect the confidentiality of that data; (2) taking steps to ensure that the Private Information that is placed in the control of its employees is restricted and limited to achieve an authorized business purpose; (3) restricting access to qualified and trained employees and/or agents; (4) designing and implementing appropriate retention policies to protect the Private Information against criminal data breaches; (5) applying or requiring proper encryption; (6) implementing multifactor authentication for access; and (7) taking other steps to protect against foreseeable data breaches.

179. Plaintiffs and Class Members would not have entrusted their Private Information to Riverside in the absence of such an implied contract.

180. Had Riverside disclosed to Plaintiffs and the Class that they did not have adequate computer systems and security practices to secure sensitive data, Plaintiffs and Class Members would not have provided their Private Information to Riverside.

181. Riverside recognized that Plaintiffs' and Class Member's Private Information is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain to Plaintiffs and the other Class Members.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
SJG STRANCH, JENNINGS & GARVEY PLLC
725-235-9750
lasvegas@stranchlaw.com

182. Riverside violated these implied contracts by failing to employ reasonable and adequate security measures to secure Plaintiffs' and Class Members' Private Information.

183. Plaintiffs and Class Members have been damaged by Riverside's conduct, including the harms and injuries arising from the Data Breach now and in the future, as alleged herein.

COUNT IV
UNJUST ENRICHMENT
(On behalf of Plaintiffs and the Nationwide Class or Alternatively Nevada Subclass)

184. Plaintiffs restate and reallege all of the allegations stated above and hereafter as if fully set forth herein.

185. This Count is pleaded in the alternative to Count III above.

186. Plaintiffs and Class Members conferred a benefit on Riverside by turning over their Private Information to Defendant and by paying for products and services that should have included cybersecurity protection to protect their Private Information. Plaintiffs and Class Members did not receive such protection.

187. Upon information and belief, Riverside funds its data security measures entirely from its general revenue, including from payments made to it by Plaintiffs and Class Members.

188. As such, a portion of the payments made by Plaintiffs and Class Members is to be used to provide a reasonable and adequate level of data security that is in compliance with applicable state and federal regulations and industry standards, and the amount of the portion of each payment made that is allocated to data security is known to Riverside.

189. Riverside has retained the benefits of its unlawful conduct, including the amounts of payment received from Plaintiffs and Class Members that should have been used for adequate cybersecurity practices that it failed to provide.

190. Riverside knew that Plaintiffs and Class Members conferred a benefit upon it, which Riverside accepted. Riverside profited from these transactions and used the Private Information of

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

Plaintiffs and Class Members for business purposes, while failing to use the payments it received for adequate data security measures that would have secured Plaintiffs' and Class Members' Private Information and prevented the Data Breach.

191. If Plaintiffs and Class Members had known that Riverside had not adequately secured their Private Information, they would not have agreed to provide such Private Information to Defendant.

192. Due to Riverside's conduct alleged herein, it would be unjust and inequitable under the circumstances for Riverside to be permitted to retain the benefit of its wrongful conduct.

193. As a direct and proximate result of Riverside's conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to (i) the loss of the opportunity to control how their Private Information is used; (ii) the compromise, publication, and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their Private Information, which remains in Riverside's possession and is subject to further unauthorized disclosures so long as Riverside fails to undertake appropriate and adequate measures to protect Private Information in its continued possession; and (vi) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

194. Plaintiffs and Class Members are entitled to full refunds, restitution, and/or damages from Riverside and/or an order proportionally disgorging all profits, benefits, and other

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

compensation obtained by Riverside from its wrongful conduct. This can be accomplished by establishing a constructive trust from which the Plaintiffs and Class Members may seek restitution or compensation.

195. Plaintiffs and Class Members may not have an adequate remedy at law against Riverside, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

COUNT V
DECLARATORY JUDGMENT
(On behalf of Plaintiffs and the Nationwide Class or Alternatively the Nevada Subclass)

196. Plaintiffs restate and reallege all of the allegations stated above and hereafter as if fully set forth herein.

197. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. Furthermore, the Court has broad authority to restrain acts that are tortious and violate the terms of the federal statute described in this Complaint.

198. Riverside owes a duty of care to Plaintiffs and Class Members, which required it to adequately secure Plaintiffs' and Class Members' Private Information.

199. Riverside still possesses Private Information regarding Plaintiffs and Class Members.

200. Plaintiffs allege that Riverside's data security measures remain inadequate. Furthermore, Plaintiffs continue to suffer injury as a result of the compromise of their Private Information and the risk remains that further compromises of their Private Information will occur in the future.

201. Under its authority pursuant to the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

a. Riverside owes a legal duty to secure its former and current employees and customers' Private Information and to timely notify former and current employees and customers of a data breach under the common law and Section 5 of the FTCA;

b. Riverside's existing security measures do not comply with its explicit or implicit contractual obligations and duties of care to provide reasonable security procedures and practices that are appropriate to protect former and current employees and customers' Private Information; and

c. Riverside continues to breach this legal duty by failing to employ reasonable measures to secure former and current employees and customers' Private Information.

202. This Court should also issue corresponding prospective injunctive relief requiring Riverside to employ adequate security protocols consistent with legal and industry standards to protect former and current employees and customers' Private Information, including the following:

a. Order Riverside to provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

b. Order that, to comply with Defendant's explicit or implicit contractual obligations and duties of care, Riverside must implement and maintain reasonable security measures, including, but not limited to:

i. engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Riverside's systems on a periodic basis, and ordering Riverside to promptly correct any problems or issues detected by such third-party security auditors;

ii. engaging third-party security auditors and internal personnel to run automated security monitoring;

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

iii. auditing, testing, and training its security personnel regarding any new or modified procedures;

iv. segmenting its user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Riverside's systems;

v. conducting regular database scanning and security checks;

vi. routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

vii. meaningfully educating its users about the threats they face with regard to the security of their Private Information, as well as the steps Riverside's former and current employees and customers should take to protect themselves.

203. If an injunction is not issued, Plaintiffs will suffer irreparable injury and will lack an adequate legal remedy to prevent another data breach at Riverside. The risk of another such breach is real, immediate, and substantial. If another breach at Riverside occurs, Plaintiffs will not have an adequate remedy at law because many of the resulting injuries are not readily quantifiable.

204. The hardship to Plaintiffs if an injunction does not issue exceeds the hardship to Riverside if an injunction is issued. Plaintiffs will likely be subjected to substantial, continued identity theft and other related damages if an injunction is not issued. On the other hand, the cost of Riverside's compliance with an injunction requiring reasonable prospective data security measures is relatively minimal, and Riverside has a pre-existing legal obligation to employ such measures.

205. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing a subsequent data breach at

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

Riverside, thus preventing future injury to Plaintiffs and other former and current employees and customers whose Private Information would be further compromised.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the Classes described above, seek the following relief:

a. An order certifying this action as a Class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiffs are proper representatives of the Nationwide Class and the Nevada Subclass as requested herein;

b. Judgment in favor of Plaintiffs and Class Members awarding them appropriate monetary relief, including actual damages, statutory damages, equitable relief, restitution, disgorgement, and statutory costs;

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;

d. An order instructing Riverside to purchase or provide funds for lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members;

e. An order requiring Riverside to pay the costs involved in notifying Class Members about the judgment and administering the claims process;

f. A judgment in favor of Plaintiffs and Class Members awarding them prejudgment and post-judgment interest, reasonable attorneys' fees, costs, and expenses as allowable by law; and

g. An award of such other and further relief as this Court may deem just and proper.

VIII. DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury on all triable issues.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

DATED: September 20, 2024

/s/ Nathan R. Ring
Nathan R. Ring
Nevada State Bar No. 12078
STRANCH, JENNINGS & GARVEY, LLC
2100 W. Charleston Boulevard, Suite 208
Las Vegas, NV 89102

Tyler J. Bean (*pro hac vice* forthcoming)
SIRI & GLIMSTAD LLP
745 Fifth Avenue, Suite 500
New York, New York 10151
Tel: (212) 532-1091
E: tbean@sirillp.com

Counsel for Plaintiff and the Proposed Class